



WEB SECURITY

30 HOURS



Hariprasanth



<https://www.linkedin.com/in/hariprasanth/>

MODULE-1 INTRODUCTION

Induction

How to get into Cybersecurity?

Career paths in Cybersecurity

What are the skills needed?

How to prepare for a job?

MODULE-2 AWARENESS TRAINING

Why Awareness Training?

CIA Triad

AAA of Security

Threats, Attacks, and Vulnerabilities

Malware

Mitigating Threats

Physical Security

MODULE-3 HACKING LAB

Introduction to Virtualization

Virtual Environment Installation

Hacking OS Installation

Hacking Tools Installation



MODULE-4 BASICS

What is HTTP?

What is DNS?

What is the Web (Pages, Browsers, Servers)?

What is URI URN URL?

What is a Subdomain?

What is a Penetration Testing?

What is Web Application Penetration Testing?

MODULE-5 LINUX BASICS


What is Linux?

Basic Linux Commands

An Overview of Terminal

Linux File Operations

Permissions and Ownership



CONTENTS

CONTENTS



MODULE-6 OWASP

OWASP

Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities (XXE)

Broken Access Control

Security Misconfiguration

Cross-Site Scripting (XSS)

Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging and Monitoring

MODULE-7 RECON

Subdomain Enumeration

Port Scanning

Screenshots

Fuzzing

Technology Analysis

MODULE-8 TESTING CMS

Testing WordPress Applications

Testing Joomla Applications

Testing Drupal Applications



MODULE-9 PENTESTING

- Live Pentest on Injection
- Live Pentest on Broken Authentication
- Live Pentest on Sensitive Data Exposure
- Live Pentest on XML External Entities (XXE)
- Live Pentest on Broken Access Control
- Live Pentest on Security Misconfiguratgaion
- Live Pentest on Cross-Site Scripting (XSS)
- Live Pentest on Insecure Deserialization
- Live Pentest on Known Vulnerabilities
- Live Pentest on Insufficient Logging & Monitoring

MODULE-10 REPORTING

- What are Pentest Reports?
- How to write Efficient Reports?
- How to submit Reports?

CONTENTS